НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

Веб-сайт: cert.gov.ru
E-mail: threats@cert.gov.ru

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТИ

VULN-20200514.7| 14 мая 2020 г.

Уровень опасности: ВЫСОКИЙ

Наличие обновления: ЕСТЬ

Удаленное выполнение кода в Adobe Acrobat и Reader

Идентификатор уязвимости	MITRE: CVE-2020-9609
Идентификатор программной ошибки	CWE-122: Переполнение буфера в динамической памяти
Описание уязвимости	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально сформированного вредоносного PDF-файла. Уязвимость обусловлена некорректным определением границ буфера памяти на основе кучи.
Категория уязвимого продукта	Прикладное программное обеспечение
Уязвимое ПО	Adobe Acrobat DC до v2020.006.20042 Adobe Acrobat Reader DC до v2020.006.20042 Adobe Acrobat до v2017.011.30166 Adobe Reader до v2017.011.30166
Рекомендации по устранению	Обновить программное обеспечение
Дата выявления	12 мая 2020 г.
Дата обновления	12 мая 2020 г.
Оценка критичности уязвимости (CVSSv3.0)	8.8 AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H
Вектор атаки (AV)	Сетевой (N)
Сложность эксплуатации уязвимости (AC)	Низкая (L)
Необходимый уровень привилегий (PR)	Отсутствует (N)
Необходимость взаимодействия с пользователем (UI)	Требуется (R)
Масштаб последствий эксплуатации уязвимости (S)	Не изменяется (U)

Влияние на конфиденциальность (C)	Высокое (H)
Влияние на целостность (I)	Высокое (H)
Влияние на доступность (A)	Высокое (H)
Степень зрелости доступных средств эксплуатации	Наличие не подтверждено
Наличие средств устранения уязвимости	Официальное решение
Достоверность сведений об уязвимости	Сведения подтверждены
Ссылки на источники	https://talosintelligence.com/vulnerability_reports/TALOS-2020-1031 https://helpx.adobe.com/security/products/acrobat/apsb20-24.html